

COMP 656 – GROUP “½ OF 5” INVESTIGATORS  
SDCCE NORTH CITY CAMPUS  
8355 Aero Dr. San Diego, CA 92123  
TEL: 619-388-1800  
EMAIL: GROUP1HALF-OF-5@SDCCD.EDU

# The Great Rhino Hunt

## Digital Forensic Report

Prepared by:

**lirai Costner**  
**Anna Liza Smith**  
**Jose Krasniansky**

Specialist Field:

**Digital Forensics**

On behalf of:

**COMP 656 – GROUP “½ OF 5” Investigators Inc.**

Subject matter:

**Module 5.9 - Digital Forensics Report**

## Table of Contents

<b>I. INTRODUCTION/ ROOT CAUSE OF THE EVENT</b> .....	<b>2</b>
<b>II. CHRONOLOGY OF EVENTS FOR INCIDENT AND RESPONSE</b> .....	<b>2</b>
<b>III. LOCATION AND DESCRIPTION OF EVIDENCE</b> .....	<b>2</b>
<b>IV. ACTIONS TAKEN BY INVESTIGATORS</b> .....	<b>3</b>
1. WHO GAVE THE ACCUSED A TELNET/FTP ACCOUNT? .....	3
2. WHAT’S THE USERNAME/PASSWORD FOR THE ACCOUNT? .....	4
3. WHAT RELEVANT FILE TRANSFERS APPEAR IN THE NETWORK TRACES? .....	4
i. <b>rhino1.jpg</b> MD5 hash: d5a83cde0131c3a034e5a0d3bd94b3c9.....	5
ii. <b>rhino2.jpg</b> MD5 hash: ed870202082ea4fd8f5488533a561b35 .....	5
iii. <b>rhino3.jpg</b> MD5 hash: b058218ea0060092d4e01ef3d7a3b815 .....	6
iv. <b>rhino4.jpg</b> MD5 hash: aa64102aff71b93ed61fb100af8d52a .....	7
v. <b>rhino5.jpg</b> MD5 hash: 1e90b7f70b2ecb605898524a88269029.....	8
4. WHAT HAPPENED TO THE HARD DRIVE IN THE COMPUTER? WHERE IS IT NOW? .....	8
5. WHAT HAPPENED TO THE USB KEY? .....	9
6. WHAT IS RECOVERABLE FROM THE DD IMAGE OF THE USB KEY? .....	9
i. <b>rhino6.jpg (password: gator)</b> MD5 hash: 6bd0e9bd4fb4a738f9ca4c351a853281.....	10
ii. <b>rhino7.jpg (password: gumbo)</b> MD5 hash: 4d37a1033450b8cc96ffd1564829d321 .....	11
iii. <b>rhino8.jpg</b> MD5 hash: d03dc23d4ec39e4d16da3c46d2932d62.....	11
iv. <b>rhino9.jpg</b> MD5 hash: 76610b7bdb85e5f65e96df3f7e417a74.....	11
v. <b>rhino10.jpg</b> MD5 hash: ca03f2eed3db06a82a8a31b3a3defa24.....	12
vi. <b>*rhino2.jpg</b> MD5 hash: ed870202082ea4fd8f5488533a561b35 .....	12
7. IS THERE ANY EVIDENCE THAT CONNECTS THE USB KEY AND THE NETWORK TRACES? IF SO, WHAT?.....	12
<b>V. ADDENDUM</b> .....	<b>13</b>
1. JOURNAL ENTRIES FOUND IN RHINOUSB.DD WORD DOCUMENT: .....	13
2. TOOLS USED FOR INVESTIGATION: .....	15
<b>VI. OTHER NOTEWORTHY EVIDENCE:</b> .....	<b>16</b>
1. PASSWORD CHANGE ATTEMPTS:.....	16
2. 2 LARGE TXT FILES WERE CARVED FROM THE USB DRIVE:.....	17
3. “GOLDEN” ACCOUNT HACK ATTEMPT: .....	19
4. RHINO.EXE:.....	20

# Digital Forensic Report

---

## I. Introduction/ Root Cause of the event

The purpose of this report is to provide corroborative evidence of the possession of rhinoceros images above the legal limit perpetrated by the suspect in the city of New Orleans. The facts and evidence presented within this report are those within the preparers' own area of expertise and knowledge and do not extend to matters and knowledge outside such expertise.

## II. Chronology of events for incident and response

The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. It has been concluded that the suspect is the primary user of this machine in question and is also pursuing his Ph.D. at the University since 1972.

Our team was immediately contacted and tasked to research the data by answering several questions to validate the crime committed by the suspect.

## III. Location and description of evidence

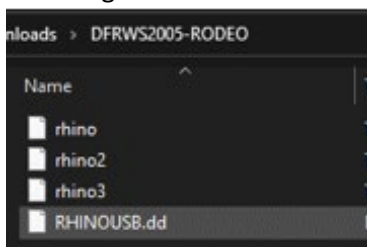
Evidence in this case includes a computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is on the CD-ROM has been provided to us.

In addition to this USB key drive image, three network traces are also available, and were provided by the network administrator and involve the machine with the missing hard drive.

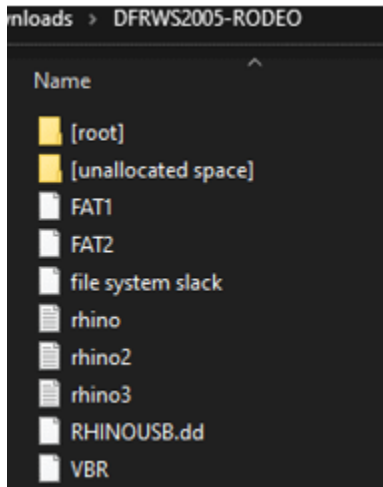
### MD5 hashes for evidence provided by network administrator:

```
c0d0093eb1664cd7b73f3a5225ae3f30 *rhino.log  
cd21eaf4acfb50f71fff857d7968341 *rhino2.log  
7e29f9d67346df25faaf18efcd95fc30 *rhino3.log  
80348c58eec4c328ef1f7709adc56a54 *RHINOUSB.dd
```

The image and trace files were provided in a zip file



Upon an initial FTK Imager extraction, more files were found:



Running a quick “file” command indicated the following file types:

rhino.log, rhino2.log, rhino3.log are PCAP files  
00004, 25604 are ASCII text (from unallocated space)  
51204 is data (from unallocated space)  
file system slack is data  
gumbo1.txt is Non-ISO extended-ASCII text  
gumbo2.txt is ISO-8859 text

#### IV. Actions taken by investigators

We have completed our main objective, which is to provide answers to questions presented by the court. The following is the list of questions, our findings/evidence, and other notes that may prove helpful or irrelevant:

##### 1. Who gave the accused a telnet/ftp account?

Evidence from the RHINOUSB.dd image revealed a Word document with metadata attached, through the Autopsy tool. This Word document lists several journal entries, where the last entry suggests that “Jeremy” gave the accused telnet/ftp account.

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

MD5 hash: Word document - 68059d3355f0138c9fdd7eaa75e7bc16

## 2. What's the username/password for the account?

After investigating a Telnet TCP Stream0, login data is:

**username:** gnome

**password:** gnome123

```
Telnet TCP Stream0:
.....#.'$......P(.....#.'$.#.$.....'..#.$..ANSI.....'
SunOS 5.9
.
.....login: .....ggnnoommee
Password: gnome12
Login incorrect
login: ggnnoommee
Password: gnome123
Last login: Mon Apr 26 16:47:47 from 137.30.122.253
```

## 3. What relevant file transfers appear in the network traces?

After changing the log files to a .pcap extension, we were able to extract the 4 following jpgs, 1 zip and 1 executable files from the network traces through FTP and HTTP transfers. Using the free tool, fcrackzip, we were able to obtain the password to contraband.zip, which revealed a 5<sup>th</sup> jpg (rhino2.jpg).

relevant file transfers		
rhino.log trace	FTP transfer	rhino1.jpg
		rhino3.jpg
rhino.log trace	HTTP transfer	contraband.zip (encrypted)
		rhino2.jpg (inside contraband.zip)
rhino2.log trace	HTTP transfer	rhino4.jpg
		rhino5.jpg
rhino3.log trace	HTTP transfer	rhino.exe

```
(kali@kali) - [~/Downloads/Rhino Hunt/Rhino Hunt files/Download-rhino-pcap/FTP]
$ fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt contraband.zip
found file 'rhino2.jpg', (size cp/uc 230448/230665, flags 1, chk 936e)

PASSWORD FOUND!!!!: pw = monkey
```

i. rhino1.jpg

MD5 hash: d5a83cde0131c3a034e5a0d3bd94b3c9



ii. rhino2.jpg

MD5 hash: ed870202082ea4fd8f5488533a561b35



iii. rhino3.jpg

MD5 hash: b058218ea0060092d4e01ef3d7a3b815



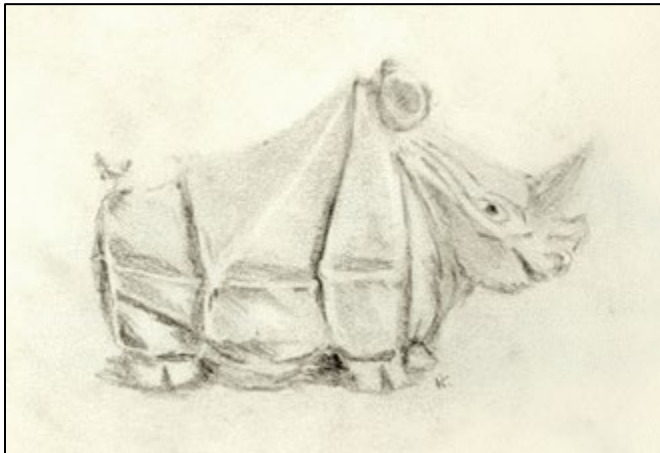
iv. rhino4.jpg

MD5 hash: aa64102afff71b93ed61fb100af8d52a



v. rhino5.jpg

MD5 hash: 1e90b7f70b2ecb605898524a88269029



#### 4. What happened to the hard drive in the computer? Where is it now?

According to the same journal entry from question 1, the suspect “threw it into the Mississippi River”.

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

Another item possibly relevant to the question is based solely on context clues from the entry. This entry may have been written shortly after the action was done. Metadata from our Autopsy tool reveals that the last modification date for this Word document is August 9, 2005:

Result: 1 of 1	
Type	Value
Organization	University of New Orleans
Date Modified	2005-08-09 11:40:00 GMT+02:00
Program Name	Microsoft Office Word
Date Created	2005-08-09 11:17:00 GMT+02:00
User ID	NOWAY MAN NO WAY MAN NO WAY.
Owner	NO WAY MAN NO WAY MAN NOWAY.
Source File Path	/img_RHINOUSB.dd/\$CarvedFiles/1/f0334472_She_died_in_February_at_the_age_of_74.doc
Artifact ID	-9223372036854775806

### 5. What happened to the USB key?

According to the same journal entry from question 1, the suspect reformatted the USB key after the entry was written (see question 4 for metadata retrieved for date), but the “good stuff” wasn’t destroyed. Action was probably performed at Radio Shack.

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I’m gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

### 6. What is recoverable from the dd image of the USB key?

There was a total of 5 rhino images that were recovered from the dd image of the USB key, 2 of which were encoded into alligator images with a password required to decode.

Notable files found:	folder:
rhino6.jpg	RHINOUSB.dd (from alligator1.jpg - pw: gator)
rhino7.jpg	RHINOUSB.dd (from alligator2.jpg - pw: gumbo)
rhino8.jpg	RHINOUSB.dd
rhino9.jpg	RHINOUSB.dd
rhino10.jpg	RHINOUSB.dd
rhino2.jpg	RHINOUSB.dd (and contraband.zip from log trace)
Word document	RHINOUSB.dd

Utilized the stegdetect tool to determine which images have this hidden image encoded, after which point, jphs tools were used to decode the alligator images.

```
D:\Downloads\DFRWS2005-RODEO\rhino\Export\Images>stegdetect *.jpg
18-f0103512.jpg : negative
Corrupt JPEG data: 8 extraneous bytes before marker 0xd9
19-f0103704.jpg : jphide(*)
20-f0104520.jpg : skipped (false positive likely)
21-f0105328.jpg : negative
22-f0105848.jpg : negative
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
23-f0105864.jpg : negative
28-f0334536.jpg : negative
f0103512.jpg : negative

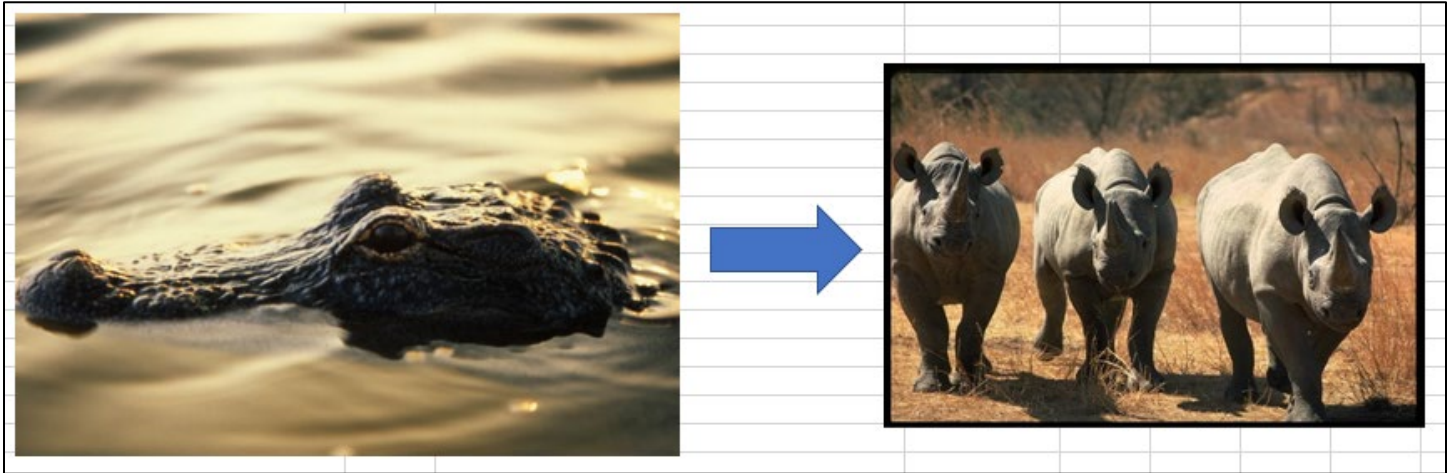
D:\Downloads\DFRWS2005-RODEO\rhino\Export\Images>stegbreak.exe -r rules.ini -t p -f 1000000-password-seclists.txt 20-f0104520.jpg
Loaded 1 files...
20-f0104520.jpg : jphide[v5](gator)
Processed 1 files, found 1 embeddings.
Time: 0 seconds: Cracks: 2736,      Inf c/s

D:\Downloads\DFRWS2005-RODEO\rhino\Export\Images>stegbreak.exe -r rules.ini -t p -f 1000000-password-seclists.txt 19-f0103704.jpg
Corrupt JPEG data: 8 extraneous bytes before marker 0xd9
Loaded 1 files...
19-f0103704.jpg : jphide[v5](gumbo)
Processed 1 files, found 1 embeddings.
Time: 1 seconds: Cracks: 15996, 15996.0 c/s
```

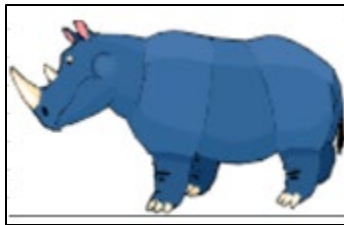
- i. rhino6.jpg (password: gator)  
MD5 hash: 6bd0e9bd4fb4a738f9ca4c351a853281



- ii. **rhino7.jpg (password: gumbo)**  
MD5 hash: 4d37a1033450b8cc96ffd1564829d321



- iii. **rhino8.jpg**  
MD5 hash: d03dc23d4ec39e4d16da3c46d2932d62



- iv. **rhino9.jpg**  
MD5 hash: 76610b7bdb85e5f65e96df3f7e417a74



v. rhino10.jpg

MD5 hash: ca03f2eed3db06a82a8a31b3a3defa24



vi. \*rhino2.jpg

MD5 hash: ed870202082ea4fd8f5488533a561b35



7. Is there any evidence that connects the USB key and the network traces? If so, what?  
Yes, **rhino2.jpg** (with same MD5 hash) was present in both the USB key and network traces.

## V. Addendum

### 1. Journal entries found in RHINOUSB.dd Word document:

She died in February at the age of 74. In August 2001 it wasn't a decision, since the alternative was regret. It wasn't her fault that I didn't go to the drugstore... And then getting her to arrange a time with Lynn, so that I can tell her just with me and Tal there.

We were walking from the restaurant to the Irish pub, and who did we run into? Then we had dinner at this really nice restaurant with a patio kind of in Old Town.

Back in March I did a presentation at a research conference held at UC Irvine and presented by the Honors Transfer Council of California.

---

My mother and I have a unique relationship. Chasing Amy - \*whimpers\* By all accounts i should have liked this film. Their relationship was a failure! All other IB families are trying to keep their kid in IB, trying to encourage their kid to do good, mine is trying to make me quit. Anyway, this one is someone she was involved with in high school who says he's been trying to find her all these years and finally tracked her down. So seeing how I am scared of pitch black darkness I got up and was trying to see what made the power go out, and my parents got up and joined me with flashlights and candles. I handed in the damn homework, which was really quite stupid for all those who do know how to use the damn computer. He turned back to me, completely sober, completely serious and replied - 'No, I don't dislike you, I'm just scared of you.' I stared at him in disbelief for a moment or two or three - scared of me?

---

There truly are buckets of phenomenal things to be amazed by, and thankful for.

Stocklos and Andrew were only there for one of the nights I was.

Then there was one 4th of July when we had just moved to a big new house in the country & we were flat busted, so we had no funds to celebrate. But Jon and been watching the encounter and remained at bay purposely in order to let me say what I had to say to Andrew. I am so excited about the trip... and so excited that Jen and Nicole are going... and so excited that we are going to both Wolves games while we are there. And she attempted lying to me about going Hong Kong together. And look, it's very difficult to work both sides of the aisle.

---

It might last. MILLER, who actually taught my HIS 102 class last semester, and he was the last class I had last time, and the first class this time.

I've been so caught up in all this craziness going on and such!

This can be a very uncomfortable moment if someone walks in and busts you.

I haven't brought it up to Amanda, but Stephen knows how uncomfortable it is. It's all uncomfortable and awkward.

And it's so easy, we're an Irish family and all that implies.

So in honor of better times: ~~heres~~ something I wrote a year ago, a moment from a night that Brady and I spent together last winter...

Sarah and I took a break after extensive arguing, where she proceeded to date my closest friend and housemate from Miami. After much haranguing from my father, my sisters, brother, ~~nieces~~ and I begrudgingly agreed to sing carols and whatnot, in unison and harmony, at our ~~huge~~ Christmas party under the name, The Family Songsters. You know, what will people remember years from now as hip?

---

All the card schools in every corner of the earth - and all that's in between - are they just a game of chance? This was foretold and all that goes along with it. I always had the feeling that he was going to turn on me one day and that I was being set up for the kill, but the moment never came. Sometimes I ~~have to~~ bribe Big Mike with a bottle of vodka to drive over in his van so I can collect an item that's too big to fit into my 13-year-old Mazda hatchback. I grunted, ~~growled~~ and prepared to tell the offending party that I was BUSY when I glanced up and saw the SN glaring at me from the new window... And then getting her to arrange a time with Lynn, so that I can tell her just with me and ~~Tal~~ there. ~~Its~~ quite a good show, although there are some problems with it: um, guys, could you lay off on the slow-motion-with-morbid-period-appropriate-soundtrack routine when tying up the end of the episode? Had a session with my therapist, Kim, on Monday as per usual. To spend some time with friends? At heart and core were a lot alike, we just get there ~~at~~ slightly different ways ~~some times~~. Science has proven that people of different races are that way because of the climate.

Not many people got the angle I did during the ceremony, to see the way they were smiling, the way that they looked at each other, but if anyone was dense enough to miss it before, they would have figured it out from seeing that. I feel, so, so what's the word... ah yes annoyed with people who think that ~~i~~ am something that I'm not when ~~i~~ barely even know them. I was told I bird walk, it means like, talking about something, going off on a tangent and talking about something completely different, then going back to what ~~i~~ was talking about before like I haven't been ranting about something else for the last 5 minutes. A complete 180 from last week and the week before, I think it has something to do with the fact I haven't seen/talked to Gus since last Tuesday.

---

In a way I don't even want to write here ~~cos~~ she might come and read it then not write herself but at the same time I've been thinking in diary entry since about 10:30pm when the distractions stopped.

I don't know what to say to him.

I don't know what I'll be feeling tomorrow night at this time, all alone with no cable and no gas and no internet access, but ~~thats~~ okay.

I still have to tell my Tom & Jerry story... probably tomorrow if I have time.

Feeling certain there was a curse upon my head, I gave up, returned home, and took a shower.

Do you have to be a gold member to put in background pics??

A little background: When I was 14, I had eye surgery to correct a birth defect. When I called them the other day to find out when they were open, I got someone very, very stern. And they sent a snotty fool down from Buffalo to run the store. However, after a while of dealing with her crap, management decided they wanted some more room in the store to put...whatever. What's the point.

Most of the rides we wanted to take were sold out, but we got to ride on a tall ship from 3-5, which is exactly what we wanted. I found this site that is full of surveys through some people who are now obsessed with the site.

---

Rhino pictures illegal? Makes me sick. I “hid” the photos... hehehehe. Apparently, if there are less than 10 photos, it's no big deal.

---

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

## 2. Tools used for investigation:

List of tools
FTK Imager stegdetect/stegbreak to jphs
Autopsy
Wireshark
fcrackzip (Linux)
stegdetect/stegbreak
jphs (jphide and jpseek)

## VI. Other noteworthy evidence:

### 1. Password change attempts:

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this [entry](#), but try not to destroy the good stuff. I need to change the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

```
cook:[gnome]$ ppaasssswwdd

passwd: Changing password for gnome
Enter existing login password: gnome123

New Password: gnome1234

passwd: Old and new passwords must differ by at least 3 positions.

Please try again
New Password: gnome12345

Re-enter new Password: gnome12345

Permission denied
cook:[gnome]$ llooggoouutt

ksh: logout: not found
cook:[gnome]$ lloogguu.. .ooouutt

ksh: logout: not found
cook:[gnome]$ eexxiitt

logout
```

2. 2 large txt files were carved from the USB drive:

The screenshot shows a file carving tool interface. On the left is a navigation pane with categories like Databases, Documents, Executable, By MIME Type, Deleted Files, MB File Size, Data Artifacts, Analysis Results, OS Accounts, and Tags. The main window is split into a 'Table' view and a 'Hex' view.

**Table View:**

Name	Location	S	C	O	Modified Time	CH
f0106360.txt	/img_RHINOUSB.dd/\$CarvedFiles/1/f0106360.txt			1	0000-00-00 00:00:00	00
f0000000.txt	/img_RHINOUSB.dd/\$CarvedFiles/1/f0000000.txt			1	0000-00-00 00:00:00	00

**Hex View:**

Page: 1 of 7129    Page:    Go to Page: 1    Jump to Offset

0x00000000:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000010:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000020:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000030:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000040:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000050:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000060:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000070:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000080:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000090:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000000a0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000000b0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000000c0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000000d0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000000e0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000000f0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000100:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000110:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000120:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000130:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000140:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000150:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000160:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000170:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000180:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x00000190:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000001a0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .
0x000001b0:	43 48 41 52 4C 49 45 0A	43 48 41 52 4C 49 45 0A	CHARLIE .CHARLIE .



3. “Golden” account hack attempt:

Telnet TCP streams show suspect trying to hack into user “Golden” ‘s account. 2 names notable:  
Georgia and John:

```
Telnet TCP Stream1:
.....#.'$. P(.....#.'$.#$. '.....#$. ANSI...'
SunOS 5.9
.
.....login: .....ggoolldeenn
Password: kkkkk
Login incorrect
login: ggoolldeenn
Password: helovessubaru
Login incorrect
login: ^D..
```

```
Telnet TCP Stream2:
.....#.'$. P(.....#.'$.#$. '.....#$. ANSI...'
SunOS 5.9
.
.....login: .....ggnnoommee
Password: gnome123
Last login: Mon Apr 26 17:23:39 from 137.30.122.253
Sun Microsystems Inc. SunOS 5.9 Generic May 2002
You have new mail.
gnome pts/8 Apr 26 17:24 (137.30.122.253)
Today is .....Mon Apr 26 17:24:34 CDT 2004
Your system identification is ...uid=2287(gnome) gid=2000(cscistu)
Your terminal address is ...../dev/pts/8
Your current directory is ...../home/gnome
Your file creation mask is .....022
Your server name is .....cook
Processor .....sparc
Operating System .....sun solaris v5.9
cook:[gnome]$ ccaatt >> JJOOHHNNRREEEAADDMMEE
Il trriieedd too hhaacckk GGoollddeenn"ss aaccccoounntt uu.. .bbuutt thhee
ppaasssswwoorrd d wwaass wwrroonngg..
----GGeoorrggee.. .iiaa
```

